

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS : Su-Hyung Kim et al.
SERIAL NO. : Not Yet Assigned
FILED : January 23, 2004
FOR : AUTHENTICATION METHOD AND APPARATUS IN EPON

PETITION FOR GRANT OF PRIORITY UNDER 35 USC 119

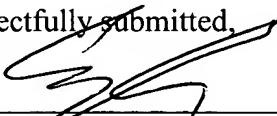
MAIL STOP PATENT APPLICATION
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA. 22313-1450

Dear Sir:

Applicant hereby petitions for grant of priority of the present Application on the basis of the following prior filed foreign Application:

<u>COUNTRY</u>	<u>SERIAL NO.</u>	<u>FILING DATE</u>
Republic of Korea	2003-14845	March 10, 2003

To perfect Applicant's claim to priority, a certified copy of the above listed prior filed Application is enclosed. Acknowledgment of Applicant's perfection of claim to priority is accordingly requested.

Respectfully submitted,


Steve S. Cha
Attorney for Applicant
Registration No. 44,069

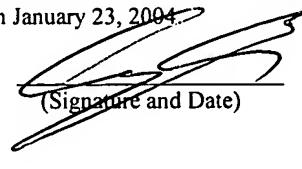
CHA & REITER
210 Route 4 East, #103
Paramus, NJ 07652
(201) 226-9245

Date: January 23, 2004

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MAIL STOP PATENT APPLICATION, COMMISSIONER FOR PATENTS, P. O. BOX 1450, ALEXANDRIA, VA. 22313-1450 on January 23, 2004.

Steve S. Cha, Reg. No. 44,069
Name of Registered Rep.)


(Signature and Date)



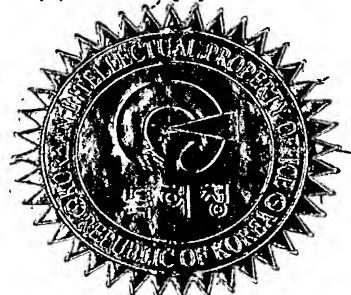
별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Intellectual
Property Office.

출 원 번 호 : 10-2003-0014845
Application Number

출 원 년 월 일 : 2003년 03월 10일
Date of Application MAR 10, 2003

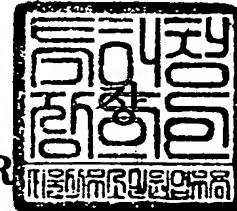
출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003 년 06 월 05 일

특 허 청

COMMISSIONER



【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0007
【제출일자】	2003.03.10
【국제특허분류】	H04L
【발명의 명칭】	E P O N에서의 인증 방법과 인증 장치과 인증 장치 및 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체
【발명의 영문명칭】	Authentication Method And Apparatus in Ethernet Passive Optical Network
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이건주
【대리인코드】	9-1998-000339-8
【포괄위임등록번호】	2003-001449-1
【발명자】	
【성명의 국문표기】	김수형
【성명의 영문표기】	KIM, SUHYUNG
【주민등록번호】	710501-1079657
【우편번호】	138-783
【주소】	서울특별시 송파구 풍납2동 우성아파트 5-706
【국적】	KR
【발명자】	
【성명의 국문표기】	김영석
【성명의 영문표기】	KIM, YOUNGSEOK
【주민등록번호】	611021-1684623
【우편번호】	463-050
【주소】	경기도 성남시 분당구 서현동 310번지 혜자촌 614-802
【국적】	KR

【발명자】

【성명의 국문표기】 오윤제
【성명의 영문표기】 OH, YUN JE
【주민등록번호】 620830-1052015
【우편번호】 449-915
【주소】 경기도 용인시 구성면 언남리 동일하이빌 102동 202호
【국적】 KR
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대
리인 이건
주 (인)

【수수료】

【기본출원료】	20	면	29,000	원
【가산출원료】	8	면	8,000	원
【우선권주장료】	0	건	0	원
【심사청구료】	0	항	0	원
【합계】	37,000			원

【요약서】

【요약】

1. 청구범위에 기재된 발명이 속하는 기술분야

본 발명은 IEEE(Institute of Electrical and Electronics Engineers) 802.3과 802.1d를 중심으로 표준화 작업이 진행될 IEEE 802에서 논의되어질 링크 보안(link Security) 방법에 관한 것임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은 OLT에서 ONU를 인증하기 위해 RADIUS 서버의 기능을 OLT에서 구현하여, OLT와 RADIUS 서버 사이의 MD-5 알고리즘을 ONU과 OLT로 단순화하여 실현하므로써 EPON 구조에서 사용할 수 있는 인증 방법 및 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있음.

3. 발명의 해결 방법의 요지

본 발명은, EPON(Ethernet Passive Optical Network)에서의 인증 방법에 있어서, OLT(Optical Line Terminal)가 ONU(Optical Network Unit)로부터 인증 절차의 시작을 알리는 패킷을 전달받아, 상기 ONU로 특성값 확인 요청 패킷을 전달하는 제 1 단계; 상기 OLT가 상기 ONU로부터 특성값을 전달받아 상기 ONU의 특성값을 확인하는 제 2 단계; 상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하면 인증 성공(Success) 패킷을 상기 ONU로 전달하는 제 3 단계; 상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하지 않으면 인증 실패(Reject) 패킷을 상기 ONU로 전달하는 제 4 단계; 및 상기 제 3 단계 또는 상기 제 4 단

계의 동작 수행 후, 상기 OLT가 상기 ONU로 인증 과정의 종료를 알리는 제 5 단계를 포함함.

4. 발명의 중요한 용도

본 발명은 EPON 등에 이용됨.

【대표도】

도 4

【색인어】

EPON, 인증, OAM, ACT, EAPOL

【명세서】**【발명의 명칭】**

E P O N에서의 인증 방법과 인증 장치와 인증 장치 및 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체{Authentication Method And Apparatus in Ethernet Passive Optical Network}

【도면의 간단한 설명】

도 1 은 종래의 기술에 따른 MD-5 챌린지를 사용한 EAP 인증 방법에 대한 일실시 예 신호 흐름도.

도 2 는 종래의 기술에 따른 CHAP 프로토콜을 이용한 인증 방법의 일실시예 신호 흐름도.

도 3 은 일반적인 EAPOL 프레임 포맷의 일실시예 구조도.

도 4 는 본 발명에 따른 EPON(Ethernet Passive Optical Network) 에서의 ONU와 OLT 간의 인증 방법에 대한 일실시예 동작 흐름도.

도 5 는 본 발명에 따른 EPON 에서의 ONU와 OLT 간의 인증 방법에 사용되는 인증 패킷의 일실시예 구조도.

도 6 은 본 발명에 따른 인증 과정을 위한 OLT의 LLID(Logical Link ID) 인증 처리 블록의 일실시예 구성도.

【발명의 상세한 설명】**【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <7> 본 발명은 IEEE(Institute of Electrical and Electronics Engineers) 802.3과 802.1d를 중심으로 표준화 작업이 진행될 IEEE 802에서 논의되어질 링크 보안(link Security)에 관한 것이다. 여기서, 링크 보안은 802.1x기반의 인증 방법과 802.10기반의 SDE(Secure Data Exchange) 구조를 포함하는 것이다. 특히, 본 발명은 EPON(Ethernet Passive Optical Network) 구조에서의 인증에 적용되며, 802.1x기반의 인증 방법을 기반으로 하여 간단하고 효과적으로 인증 방법을 구현하도록 하기 위한 방법이다.
- <8> IEEE 802.1x(port-based network control)에서는 각각 단말과 Bridged-LAN 장비 사이에서의 인증 프로토콜(EAP over Ethernet, EAPOL)과 Bridged-LAN 장비와 RADIUS(Remote Authentication Dial-In User Services) 서버 사이의 프로토콜(EAP over RADIUS, RFC2869)이 모두 지원되고 있다.
- <9> 이와 같은 현재의 구조로 인증을 수행하려면 RADIUS 서버를 외부에 설치해야 한다. 또한, 무선(Wireless)-Lan에서는 가입자에 대한 인증을 수행하기 위해 IEEE 802.1x에서 제안된 인증 프로토콜을 사용하고 있다. 현재 인증 프로토콜로 써는 PAP(Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol), EAP(Extended Authentication Protocol) 등이 사용되고 있고, PDU부분의 암호화를 위한 해쉬 기능을 위해 MD-5알고리즘을 사용한다. 즉, 인증자와 RADIUS서버 사이에서 MD-5 라

는 알고리즘을 사용하여 RADIUS 프레임 내의 패스워드 등에 대한 암호화를 수행하고 있는 것이다.

<10> 도 1 은 종래의 기술에 따른 MD-5 챌린지를 사용한 EAP 인증 방법에 대한 일실시예 신호 흐름도이다. 도 1 에 도시된 바와 같이, 일반적인 EAP 인증을 위한 시스템은 클라이언트인 PC(Personal Computer)(11), 인증을 위한 인증 서버(13) 및 네트워크 액세스를 위한 NAS(Network Access Server)(12)를 포함하여 구성되며, 그 신호 흐름은 다음과 같다.

<11> 우선, PC(11)와 NAS(12) 사이에서 인증을 위한 프로토콜을 결정한다(101). 여기서, NAS(12)는 단순히 인증서버(13)로의 릴레이 동작만을 수행하고, 인증 서버(13)와 PC(11) 간의 인증 결과를 이용해서 포트의 사용을 허가한다. 본 실시예에서는 EAP 인증을 선택한다.

<12> 그리고, PC(11)는 인증 서버(13)로 사용자 이름(Username)을 이용한 EAP 인증을 시도한다(102). 이러한 인증 시도에 대해 인증 서버(13)는 해쉬 함수를 위한 챌린지 값이 포함된 MD-5 챌린지를 PC(11)로 전송한다(103).

<13> 그리고, PC(11)는 인증 서버(13)로 해쉬 값을 포함한 MD-5 응답(Response)을 전달한다(104). 전달된 MD-5 응답(Response)이 맞으면, 인증은 성공한 것으로 인증 서버(13)는 인증 성공 메시지를 전송하고(105), 이후 NAS(12)를 통해 목적지 주소와 연결된다.

<14> 한편, PC(11)는 인증 서버(13)로 해쉬 값을 포함한 MD-5 응답(Response)을 전달한다. 전달된 MD-5 응답(Response)이 맞지 않으면, 인증은 실패한 것으로 인증 서버(13)는 인증 실패 메시지를 전송하고(105), 해당 PC(11)의 접속은 거부된다.

- <15> 도 2 는 종래의 기술에 따른 CHAP 프로토콜을 이용한 인증 방법의 일실시예 신호 흐름도이다. 여기서, CHAP은 MD-5 CHAP 이라고도 하며 챌린지(Challenge)-응답(response) 방식의 인증 프로토콜이다. CHAP은 산업 표준 MD-5 단방향 구성표를 사용하여 응답을 암호화하여 무단 액세스에 대해 높은 수준의 보안을 제공한다. 인증 프로세스는 도 2 에 도시된 바와 같다.
- <16> 즉, 액세스 클라이언트인 PC(21)가 사용자 이름(Username)을 이용해서 RADIUS 서버(22)에 로그온(Log-On)하면(201), RADIUS 서버(22)는 세션 ID와 임의의 챌린지(Challenge) 문자열로 구성되는 CHAP 챌린지를 PC(21)에 전달한다(202).
- <17> 그리고, PC(21)는 사용자 이름 및 챌린지 문자열의 단방향 암호화, 세션 ID 및 암호가 들어 있는 CHAP 응답(Response) 메시지를 보낸다(203).
- <18> 그리고, RADIUS 서버(22)는 CHAP 응답(Response) 메시지를 확인하여 유효하면 CHAP 성공 메시지를 전달해서(204) 연결을 허용한다.
- <19> 도 3 은 일반적인 EAPOL 프레임 포맷의 일실시예 구조도이다.
- <20> 일반적인 EAPOL 프레임 포맷은 목적지 주소(DA : Destination Address)(301), 소스 주소(SA : Source Address)(302), Etype(303), 버전(304), 패킷 타입(305), 패킷 바디 길이(306) 및 패킷 바디(307)로 구성된다.
- <21> 여기서, Etype(303) "0x88-8e"를 사용하는 EAP의 프레임 구조를 보여 주고 있다. 그러나, 이러한 이더 타입 "0x88-8e"는 현재 무선 Lan에서 사용 중이므로 다른 이더 타입이 사용되어야 한다.

- <22> 한편, EPON은 IEEE 802 표준화 기구에서 가장 활발한 표준화 대상으로서, 기존의 이더넷망과 달리 점 대 다수점(point-to-multipoint) 형상의 광 통신망에서 동작한다. 이러한 EPON은 점 대 점(Point-to-point) 방식에 비하여, 경제적인 장점이 있으며, 현재 MPCP(Multi Point CONUrol Protocol)라고 불리는 중앙 집중형 MAC(media access cONUrol) 제어 프로토콜과 EPON 상에서의 점 대 점 전달을 에뮬레이션(emulation)하는 기법에 대한 연구가 활발하다. 또한, 이러한 EPON에 있어서도 보안이 문제가 되는데, 현재, EPON 구조에서 대상 단말에 대한 인증 방법은 표준화에 정의되어 있는 것이 없다. 다만, 포트별 제어 구조를 갖는 IEEE802.1x가 향후 표준적인 인증 방법의 기본 방향이 될 것으로 보인다. 따라서, EPON 구조에서 사용할 수 있는 인증 프로토콜의 설계가 필요로 하다.
- <23> 이를 위한 상기 도 1 및 도 2에서 제시하는 종래의 인증 방법은 여러가지 문제점을 안고 있다.
- <24> 첫번째, 소수의 ONU(Optical Network Unit)을 인증하는데, 기존 RADIUS 서버를 이용한 구조는 외부에 인증을 위한 서버를 따로 구축하는 등 운용 비용이나 구현 방법 등에서 불필요한 구조를 가지고 있다.
- <25> 두번째, ONU(Optical Network Unit)와 OLT(Optical Line Terminal)사이에 EAP를 사용하기 곤란하다. ONU에 기존 사용 중인 이더넷 타입을 중복해서 사용하는 경우, 상기의 도 3에서 보여졌듯이, 무선 랜과 EPON의 인증을 위한 "Etype"이 같아서 그 구분이 되지 않는 문제가 있다. 따라서, 기존 이더넷 타입이 아닌 새로운 이더 타입이나 구현하기 쉬운 새로운 포맷의 프레임이 필요하다.
- <26> 세번째, ONU와 OLT의 인증 프로토콜을 변경 내지 단순화하여야 한다.

<27> 네번째, 종래 기술인 IEEE 802.1X구조에서는 브릿지 기반의 포트제어 기능을 기반으로 하므로, LLID(Logical Link ID)를 포트 제어에 이용해야 하는 EPON 구조에는 사용 할 수 없다.

【발명이 이루고자 하는 기술적 과제】

<28> 본 발명은, 상기와 같은 문제점을 해결하기 위하여 제안된 것으로, OLT에서 ONU를 인증하기 위해 RADIUS 서버의 기능을 OLT에서 구현하여, OLT와 RADIUS 서버 사이의 MD-5 알고리즘을 ONU과 OLT로 단순화하여 실현하므로써 EPON 구조에서 사용할 수 있는 인증 방법과 인증 장치 및 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는데 그 목적이 있다.

<29> 또한, 본 발명은, 종래의 구조에서는 포트를 제어하기 위해서는 MAC 어드레스 등을 사용하여야 하지만, 패스워드와 LLID 매핑 테이블을 이용한 포트 제어가 가능하도록 하는 데 그 목적이 있다.

【발명의 구성 및 작용】

<30> 상기의 목적을 달성하기 위한 본 발명은, EPON(Ethernet Passive Optical Network)에서의 인증 방법에 있어서, OLT(Optical Line Terminal)가 ONU(Optical Network Unit)로부터 인증 절차의 시작을 알리는 패킷을 전달받아, 상기 ONU로 특성값 확인 요청 패킷을 전달하는 제 1 단계; 상기 OLT가 상기 ONU로부터 특성값을 전달받아 상기 ONU의 특성값을 확인하는 제 2 단계; 상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT

에 사전에 저장된 값과 일치하면 인증 성공(Success) 패킷을 상기 ONU로 전달하는 제 3 단계; 상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하지 않으면 인증 실패(Reject) 패킷을 상기 ONU로 전달하는 제 4 단계; 및 상기 제 3 단계 또는 상기 제 4 단계의 동작 수행 후, 상기 OLT가 상기 ONU로 인증 과정의 종료를 알리는 제 5 단계를 포함한다.

<31> 또한, 본 발명은, EPON(Ethernet Passive Optical Network)에서의 인증 방법에 있어서, ONU(Optical Network Unit)가 OLT(Optical Line Terminal)로 인증 절차의 시작을 알리는 패킷을 전달하고, 상기 ONU로부터 특성값 확인 요청 패킷을 전달받는 제 1 단계; 상기 ONU가 상기 OLT로 특성값을 전달하여 상기 ONU의 특성값을 확인 받는 제 2 단계; 상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하면 인증 성공(Success) 패킷을 상기 ONU로 전달하는 제 3 단계; 상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하지 않으면 인증 실패(Reject) 패킷을 상기 ONU로 전달하는 제 4 단계; 및 상기 제 3 단계 또는 상기 제 4 단계의 동작 수행 후, 상기 ONU가 상기 OLT로부터 인증 과정의 종료를 알리는 패킷을 전달받는 제 5 단계를 포함한다.

<32> 한편, 본 발명은, EPON에서의 인증 장치에 있어서, 외부의 라우터와 데이터 입출력을 하기 위한 버스 인터페이스; 인증에 따른 OAM 패킷을 받아 ONU에 대한 데이터 서비스를 제어하기 위한 제어부; 및 상기 제어부의 제어에 따라, 상기 버스 인터페이스를 통해 전달된 데이터를 스위칭하는 다운 스트림부를 포함한다

<33> 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다. 또한, 본 발명을 설명함에 있어서, 관련된 공지기능 혹은 구성에 대한 구체적인 설

명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명은 생략한다.

<34> IEEE 802.1x에서는 각각 단말과 Bridged-LAN 장비 사이에서의 인증 프로토콜(EAP over Ethernet, EAPOL)과 Bridged-LAN(NAS) 장비와 RADIUS(Remote Authentication Dial-In User Services) 서버 사이의 프로토콜(EAP over RADIUS, RFC2869)을 모두 구현하고 있지만, 본 발명은 RADIUS 기능을 OLT로 구현하는 것이다.

<35> 따라서, 본 발명에 따른 새로운 인증 방법은 도 4에서 정의된 방법과 같다.

<36> 도 4는 본 발명에 따른 EPON(Ethernet Passive Optical Network)에서의 ONU와 OLT 간의 인증 방법에 대한 일실시예 동작 흐름도이다. 도 4에 도시된 바에 따르면, 우선 ONU는 인증 절차의 시작을 알리는 패킷을 OLT로 보낸다(401). 여기서, ONU와 OLT 간의 패킷은 새롭게 정의된다. 이에 대한 상세한 정의는 후술하는 도 5의 설명에서 좀 더 상세히 살펴보기로 한다. 이때, 패킷의 코드값을 인증 동작의 시작을 표시하는 "Start"를 의미하는 값을 취한다.

<37> 그리고, 인증 동작의 시작에 따라 OLT는 ONU로 사용자 이름(Username) 확인 요청 패킷을 전달한다(402). 이때, 패킷의 코드값은 사용자 이름(Username) 확인 요청을 표시하는 "Request"를 의미하는 값을 갖는다.

<38> 그리고, ONU는 사용자 이름을 OLT로 전달하여 응답한다(403). 이때, 패킷의 코드값은 응답임을 표시하는 "Response"를 의미하는 값을 갖는다.

<39> 그리고, OLT는 ONU가 인증 패킷에 실어보낸 ONU의 특성값(본 실시예에서는 Username)을 확인한다. 그리고, 해당 ONU가 유효한 "Username"이라면, 인증 성공

(Success) 패킷을 보낸다(404). 한편, 해당 ONU가 유효한 "Username"이 아니라면 즉시 인증 실패(Access Reject) 패킷을 보낸다(404).

<40> 그리고, 인증 성공 또는 실패 후(404), OLT는 ONU로 인증 과정의 종료를 알리는 패킷을 전송한다(405). 이 패킷의 코드는 인증 종료(END)를 의미하는 값을 가진다.

<41> 도 5 는 본 발명에 따른 EPON 에서의 ONU와 OLT 간의 인증 방법에 사용되는 인증 패킷의 일실시예 구조도이다. 도 5 에 도시된 바와 같이, 본 발명에 따른 EPON 에서의 ONU와 OLT 간의 인증 방법에 사용되는 인증 패킷은 목적지 주소(DA : Destination Address)(501), 소스 주소(SA : Source Address)(502), LLID(503), 타입(504), 서브 타입(505), 버전(506), 코드(507), 데이터/PDU(protocol data unit)(508) 및 FCS(509)로 구성된다.

<42> 즉, 패킷의 목적지를 표시하는 목적지 주소(DA : Destination Address) 필드(501), 패킷의 출발점을 표시하는 소스 주소(SA : Source Address) 필드(502), 논리 링크 식별자를 표시하는 LLID 필드(503), 패킷의 이더 타입을 표시하는 타입 필드(504), 타입 필드(504)가 같은 경우 패킷의 식별을 하기 위한 서브 타입 필드(505), 패킷의 버전 정보를 표시하기 위한 버전 필드(506), 패킷의 인증 동작을 표시하기 위한 코드 필드(507), 패킷의 데이터를 표시하기 위한 데이터/PDU(protocol data unit)(508) 및 데이터 통신에서 정보를 프레임별로 나누어 전송할 때 각 프레임의 끝에 오류 검출을 위한 FCS(frame check sequence) 필드(509)를 포함한다.

<43> 특히, 도 5 의 인증 패킷은 기존 OAM(Operation, Administration, and Maintenance) 프레임을 이용한 새로운 프레임 포맷(서브 타입 0x04)을 보여 주고 있다. IEEE 802.3ah에서는 서브 타입

"0x04"를 사용하지 않고 있으므로 다른 이더 타입이 확장되기 전까지도 사용하는데 무리가 없다.

<44> 즉, 본 발명에 따른 인증 패킷은 ONU의 무선 랜으로의 기능 확장(Etype=0x888e)을 고려하여 "Etype"만으로 사용하지 않고, IEEE 802.3ah EFM에서 정의된 OAM프레임(서브 타입=0x04)을 추가 확장하여 사용한다. 따라서, 무선 랜의 "Etype"과 EPON 인증 패킷의 "Etype"이 같아서 생기는 오류의 위험을 서브 타입(505)을 이용해 피할 수 있다.

<45> 그리고, 코드 필드(506)는 인증 패킷의 동작을 나타내는 것으로 각각의 동작은 하기 <표 1>과 같다.

<46> 【표 1】

코드	내용	
0x00	Start	인증 프로세스 시작
0x01	Request	인증 내용(LLID) 요구
0x02	Response	인증 내용(LLID) 전송
0x03	End	인증 프로세스 끝
0x04	AutResult Access Accept	인증 성공
0x05	AutResult Access Reject	인증 실패

<47> 이러한 인증 과정에 의해, EPON의 OLT에서 ONU에 대한 인증을 수행하게 되는데, OLT에서 보면, ONU에 대한 초기 등록 과정 후, 하향으로는(OLT->ONU) 인증되지 않는 ONU에 대해서 데이터 서비스를 제공하지 않고, 상향으로는(ONU->OLT) 포트레벨의 제어기능을 이용하여 특정 서버에의 포트에 대해 플러딩(flooding)공격 등을 방지하기 위해, OLT에는 인증 절차에 필요한 기능을 처리하는 처리 블록이 필요하다.

<48> 이와 같이 본 발명에 따른 인증 과정을 위한 OLT의 LLID(Logical Link ID) 인증 처리 블록의 일실시예 구성도는 도 6과 같다. 도 6에 도시된 바와 같이, 본 발명에 따른

LLID 인증 처리 블록은 외부의 라우터(61)와 데이터 입출력을 하기 위한 버스 인터페이스(62), 인증에 따른 OAM 패킷을 받아 ONU에 대한 데이터 서비스를 제어하기 위한 제어부(64) 및 제어부(64)의 제어에 따라 버스 인터페이스(62)를 통해 전달된 데이터를 스위칭하는 다운 스트림부(63)를 포함한다.

<49> 여기서, 제어부는 도 5의 본 발명에 따른 새로운 OAM 프레임을 입력받아 "ALTM(Address Lockup Table Management)+ACT(Authentication CONUrol Table)"에 따라 다음 스트림부의 포트의 스위칭 동작을 제어한다.

<50> 여기서, ALTM을 사용하는 이유는, ALTM을 사용하면 점 대 다중점 PON 구조에서도 마치 공유(shared) LAN 구조에서와 같이 ONU 들간의 통신을 가능하게 해줄 수 있기 때문이다. 그리고, ALT는 주로 CAM(Contents Address Memory)를 이용하여 구현한다.

<51> ALTM블록에 대한 기능을 좀 더 상세히 기술하면, OLT에 연결되어 있는 ONU에서 데이터를 전송할때는 LLID를 삽입하여 OLT로 전송하게 된다. 이때 OLT에서는 DA(Destination MAC Address)를 OLT가 가지고 있는 ALT에서 룩업(Lookup)하여 OLT내에 있는 스테이션일 경우 OLT외부로 보내지 않고 LLID를 변경하여 전송한다. 여기에서 ALTM 블록은 수신된 프레임에서 SA 필드를 새롭게 변경 또는 삭제하는 기능을 한다.

<52> 위의 기능을 사용하면 학습(Learning) 과정에서 완성된 테이블을 룩업(Lookup)하여 OLT이하의 ONU 들에 대한 MAC 어드레스를 기본으로 하여 변경된 LLID를 ONU 들로 재전송 할 수 있고 필터링 기능을 이용해서 해당 ONU만 자신에게 수신되는 프레임을 받을 수 있다. 이로써 ONU 들간의 통신이 가능하게 되는 것이다.

<53> 그리고, ACT는 초기 등록 후, ONU들은 OLT 스케줄러를 통해 할당받은 LLID와 자신의 MAC 어드레스를 OLT의 ALT에 초기값을 입력 시킨 상태에서 자신을 인증해 줄 것을 OLT에 요청하는 시작(Start) 프레임을 보내게 되는데 사용자 이름(Username)에 자신의 Mac 어드레스등을 적어 보내 OLT로 하여금 인증에 필요한 파라메터로 사용하게 한다.

<54> 또한, ACT에서는 응답(Response) 프레임을 통해 새롭게 입력된 LLID를 가지고 기존의 ALT에서 할당되었던 미리 할당된 LLID와 MAC 어드레스를 비교하여 일치하는 경우만 포트를 제어하여 서비스가 이루어 지도록 한다.

<55> 이러한 "ALTM(Address Lockup Table Management)+ACT(Authentication CONUrol Table)"에 따라 본 발명에서의 동작을 상세히 살펴보면, 먼저 제어부는 OAM 프레임을 입력받는데, "Start" 프레임에서 "사용자 이름(Username)"이 OLT에 미리 설정된 값과 동일하면 "리퀘스트(Request)" 프레임을 보내면서 다운스트림부에 프레임의 LLID를 입력한다. 그리고, ONU로부터의 "응답(Response)" 프레임을 통해 인증이 성공하면 포트 일치 신호를 통해 해당 LLID의 포트는 정상 상태로 연결된다. 그러나, 만일 일치하지 않으면 포트 불일치 신호를 보내어 해당 포트를 해제한다.

<56> 이때 사용되는 ACT 의 예는 다음의 <표 2>와 같다.

<57> 【표 2】

LLID 입력	사전에 정의된 인증 LLID	인증 결과	MAC 주소
---------	--------------------	-------	--------

<58> 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 형태로 기록매체(씨디롬, 램, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다.

<59> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

【발명의 효과】

<60> 상기와 같은 본 발명은, EPON에서 ONU를 인증하기 위한 간단한 프로토콜을 제공하여, 무선 랜파의 이더 타입의 충복 문제를 피해 인증 프로토콜을 구현할 수 있는 효과가 있다.

<61> 또한, RADIUS 서버를 구현하지 않고도 기존에서 사용하는 알고리즘을 사용할 수 있으며, LLID(Logical Link ID)를 이용한 포트제어 방식으로 인증 방법을 구체적으로 구현하는 효과가 있다.

【특허 청구범위】**【청구항 1】**

EPON(Ethernet Passive Optical Network)에서의 인증 방법에 있어서,
OLT(Optical Line Terminal) 가 ONU(Optical Network Unit)로부터 인증 절차의 시
작을 알리는 패킷을 전달받아, 상기 ONU로 특성값 확인 요청 패킷을 전달하는 제 1
단계;
상기 OLT가 상기 ONU로부터 특성값을 전달받아 상기 ONU의 특성값을 확인하는 제 2
단계;
상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값
과 일치하면 인증 성공(Success) 패킷을 상기 ONU로 전달하는 제 3 단계;
상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과
일치하지 않으면 인증 실패(Reject) 패킷을 상기 ONU로 전달하는 제 4 단계; 및
상기 제 3 단계 또는 상기 제 4 단계의 동작 수행 후, 상기 OLT가 상기 ONU로 인증
과정의 종료를 알리는 제 5 단계를 포함하는 EPON에서의 인증 방법.

【청구항 2】

제 1 항에 있어서,
상기 ONU의 특성값은 사용자 이름(Username)인 것을 특징으로 하는 EPON에서의 인
증 방법.

【청구항 3】

제 1 항 또는 제 2 항에 있어서,

상기 EPON에서의 인증 방법에 사용되는 패킷은,

상기 패킷의 목적지를 표시하는 목적지 주소(DA : Destination Address) 필드;

상기 패킷의 출발점을 표시하는 소스 주소(SA : Source Address) 필드;

논리 링크 식별자를 표시하는 LLID 필드;

상기 패킷의 이더 타입을 표시하는 타입 필드;

상기 타입 필드가 같은 경우, 상기 패킷의 식별을 하기 위한 서브 타입 필드;

상기 패킷의 버전 정보를 표시하기 위한 버전 필드;

상기 패킷의 인증 동작을 표시하기 위한 코드 필드;

패킷의 데이터를 표시하기 위한 데이터/ PDU(protocol data unit); 및

데이터 통신에서 정보를 프레임별로 나누어 전송할 때 각 프레임의 끝에 오류 검출을 위한 FCS(frame check sequence) 필드를 포함하여 구성되는 것을 특징으로 하는 EPON에서의 인증 방법.

【청구항 4】

제 3 항에 있어서,

상기 코드 필드는,

인증 프로세서의 시작을 표시하는 "0x00", 인증 내용을 요구하기 위한 "0x01", 인증 내용의 전송을 표시하는 "0x02", 인증 프로세스의 종료를 표시하는 "0x03", 인증 성공

을 표시하는 "0x04" 및 인증 실패를 표시하는 "0x05" 값을 가지는 것을 특징으로 하는 EPON에서의 인증 방법.

【청구항 5】

EPON(Ethernet Passive Optical Network)에서의 인증 방법에 있어서, ONU(Optical Network Unit) 가 OLT(Optical Line Terminal)로 인증 절차의 시작을 알리는 패킷을 전달하고, 상기 ONU로부터 특성값 확인 요청 패킷을 전달받는 제 1 단계; 상기 ONU가 상기 OLT로 특성값을 전달하여 상기 ONU의 특성값을 확인받는 제 2 단계; 상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하면 인증 성공(Success) 패킷을 상기 ONU로 전달하는 제 3 단계; 상기 제 2 단계의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하지 않으면 인증 실패(Reject) 패킷을 상기 ONU로 전달하는 제 4 단계; 및 상기 제 3 단계 또는 상기 제 4 단계의 동작 수행 후, 상기 ONU가 상기 OLT로부터 인증 과정의 종료를 알리는 패킷을 전달받는 제 5 단계를 포함하는 EPON에서의 인증 방법.

【청구항 6】

제 5 항에 있어서,

상기 ONU의 특성값은 사용자 이름(Username)인 것을 특징으로 하는 EPON에서의 인증 방법.

【청구항 7】

제 5 항 또는 제 6 항에 있어서,
상기 EPON에서의 인증 방법에 사용되는 패킷은,
상기 패킷의 목적지를 표시하는 목적지 주소(DA : Destination Address) 필드;
상기 패킷의 출발점을 표시하는 소스 주소(SA : Source Address) 필드;
논리 링크 식별자를 표시하는 LLID 필드;
상기 패킷의 이더 타입을 표시하는 타입 필드;
상기 타입 필드가 같은 경우, 상기 패킷의 식별을 하기 위한 서브 타입 필드;
상기 패킷의 버전 정보를 표시하기 위한 버전 필드;
상기 패킷의 인증 동작을 표시하기 위한 코드 필드;
패킷의 데이터를 표시하기 위한 데이터/PDU(protocol data unit); 및
데이터 통신에서 정보를 프레임별로 나누어 전송할 때 각 프레임의 끝에 오류 검출
을 위한 FCS(frame check sequence) 필드를 포함하여 구성되는 것을 특징으로 하는 EPON
에서의 인증 방법.

【청구항 8】

제 7 항에 있어서,

상기 코드 필드는,

인증 프로세서의 시작을 표시하는 "0x00", 인증 내용을 요구하기 위한 "0x01", 인증 내용의 전송을 표시하는 "0x02", 인증 프로세스의 종료를 표시하는 "0x03", 인증 성공을 표시하는 "0x04" 및 인증 실패를 표시하는 "0x05" 값을 가지는 것을 특징으로 하는 EPON에서의 인증 방법.

【청구항 9】

EPON에서의 인증 장치에 있어서,

외부의 라우터와 데이터 입출력을 하기 위한 버스 인터페이스;

인증에 따른 OAM 패킷을 받아 ONU에 대한 데이터 서비스를 제어하기 위한 제어부;

및

상기 제어부의 제어에 따라, 상기 버스 인터페이스를 통해 전달된 데이터를 스위칭 하는 다운 스트림부를 포함하는 EPON에서의 인증 장치.

【청구항 10】

제 9 항에 있어서,

상기 제어부는, OAM 프레임을 입력받아 "ALTM+ACT(Authentication CONUrol Table)"에 따라, LLID를 이용하여 상기 다운 스트림부의 하향 포트의 스위칭 동작을 제어하는 것을 특징으로 하는 EPON에서의 인증 장치.

【청구항 11】

프로세서를 구비한 EPON의 OLT에,

OLT(Optical Line Terminal) 가 ONU(Optical Network Unit)로부터 인증 절차의 시작을 알리는 패킷을 전달받아, 상기 ONU로 특성값 확인 요청 패킷을 전달하는 제 1 기능;

상기 OLT가 상기 ONU로부터 특성값을 전달받아 상기 ONU의 특성값을 확인하는 제 2 기능;

상기 제 2 기능의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하면 인증 성공(Success) 패킷을 상기 ONU로 전달하는 제 3 기능;

상기 제 2 기능의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하지 않으면 인증 실패(Reject) 패킷을 상기 ONU로 전달하는 제 4 기능; 및

상기 제 3 기능 또는 상기 제 4 기능의 동작 수행 후, 상기 OLT가 상기 ONU로 인증 과정의 종료를 알리는 제 5 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【청구항 12】

프로세서를 구비한 EPON의 ONU에,

ONU(Optical Network Unit) 가 OLT(Optical Line Terminal)로 인증 절차의 시작을 알리는 패킷을 전달하고, 상기 ONU로부터 특성값 확인 요청 패킷을 전달받는 제 1 기능;

상기 ONU가 상기 OLT로 특성값을 전달하여 상기 ONU의 특성값을 확인받는 제 2 기능;

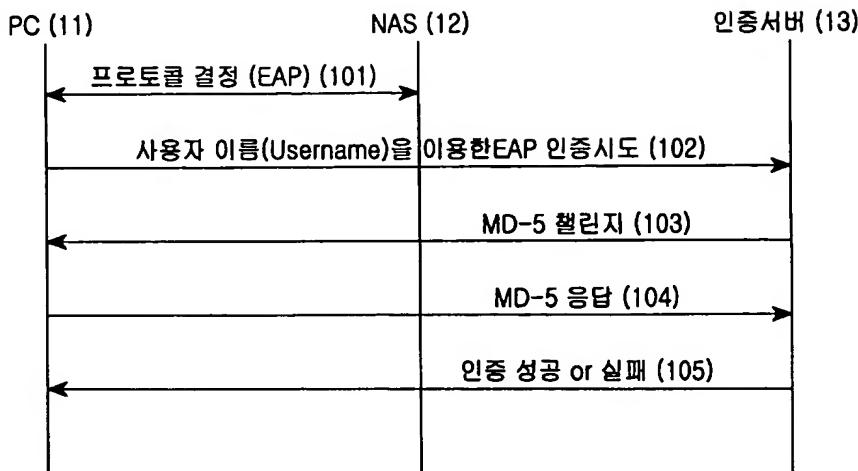
상기 제 2 기능의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하면 인증 성공(Success) 패킷을 상기 ONU로 전달하는 제 3 기능;

상기 제 2 기능의 확인 결과, 상기 ONU의 특성값이 상기 OLT에 사전에 저장된 값과 일치하지 않으면 인증 실패(Reject) 패킷을 상기 ONU로 전달하는 제 4 기능; 및

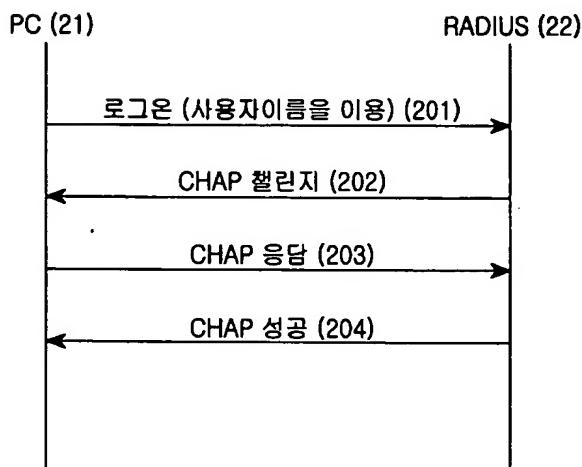
상기 제 3 기능 또는 상기 제 4 기능의 동작 수행 후, 상기 ONU가 상기 OLT로부터 인증 과정의 종료를 알리는 패킷을 전달받는 제 5 기능을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

【도 1】



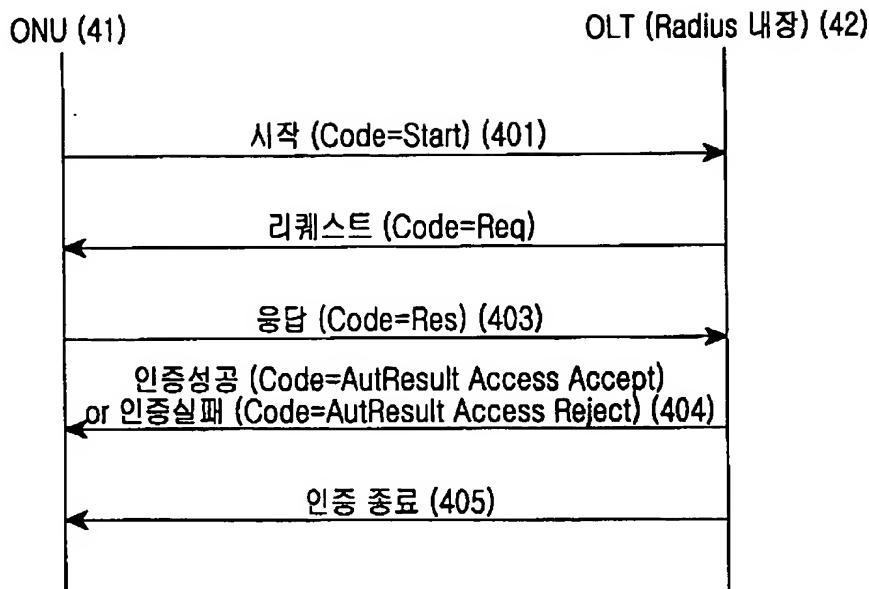
【도 2】

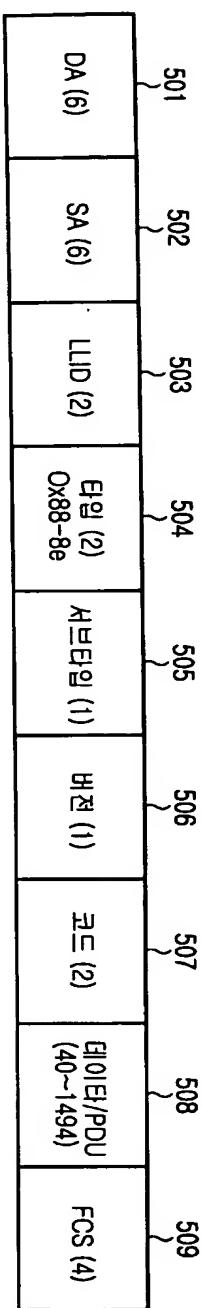


【도 3】

301	302	303	304	305	306	307
DA (6)	SA (6)	EType (2) 0x88-8e	버전 (1)	페킷타입 (1)	페킷바디길이 (2)	페킷바디

【도 4】



【5】

【도 6】

